

**IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division**

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
EMAIL ACCOUNT:

naamcommodities@gmail.com

THAT IS STORED AT PREMISES
CONTROLLED BY GOOGLE LLC

Case No. 3:23-sw-

119

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT**

I, Nathan Denny, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with the email account naamcommodities@gmail.com ("Target Account") that is stored at premises owned, maintained, controlled, and operated by Google LLC ("Google"), an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

2. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Google to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

3. Your Affiant is a Special Agent with the Federal Bureau of Investigation (“FBI”) currently assigned to the Richmond Field Office in Richmond, Virginia. I have been employed with the FBI since 2021. I am currently assigned to work investigations of complex financial crimes. I am a graduate of the FBI Training Academy in Quantico, Virginia where I received training in white-collar crime, cyber-crime, interviewing and interrogations, evidence collecting, intelligence analysis, and legal matters, among other investigative subjects. By virtue of my FBI employment, I have performed a variety of investigative tasks, including conducting arrests and executing federal search warrants. As part of my duties with the FBI, I investigate violations of federal law, including wire fraud, mail fraud, bank fraud, securities fraud, conspiracy, money laundering, and health care fraud.

4. I am a “federal law enforcement officer” within the meaning of Rule 41(a)(2)(C) of the Federal Rules of Criminal Procedure, and I am authorized to execute warrants issued under the authority of the United States.

5. The facts set forth in this affidavit are based upon my training and experience, my personal knowledge of this investigation, and my review of records, documentation, and information provided to me from others, including email correspondence, financial and business records, and in-person interviews.

6. Since this affidavit is being submitted for the limited purpose of securing a search warrant, the information within is limited in scope to the information relevant to this purpose, and I have not included every fact known to me or others concerning this investigation. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant.

7. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 18 U.S.C. § 1343 (wire fraud) have been committed

by Naveed Arshad. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

8. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

9. Naveed Arshad, a resident of Richmond, Virginia, is the sole owner of a company called Naam Commodities FZ LLC (“Naam”), which is registered in Virginia and operates in the Ras Al Khaimah Economic Free Zone in the United Arab Emirates (UAE). According to its website, Naam is a global commodity trading entity, specializing in soft commodities such as corn, wheat, sugar, and rice, and non-ferrous metals such as aluminum, copper, and zinc. According to information obtained from the Virginia State Corporation Commission, Naam was registered by Arshad in Virginia on April 19, 2021.

10. As explained below, Arshad devised and executed a scheme to fraudulently obtain funds from acquaintances and business associates with no intention of using the funds for the agreed upon purpose and with no intention of repaying the funds or any of the promised dividends.

Futures Contract with D.B.

11. In early 2022, a mutual associate introduced Arshad to a commodity trading business owner, D.B., who was looking for a soybean seller for two large futures contracts with companies in China. The first contract was worth \$575,000, the second was worth \$5.6 million.

Arshad agreed to be the supplier for these transactions and provided quotes to D.B.'s company for the two contracts. The final agreement was signed by both parties on January 17, 2022. The terms of this contract included the following statement: "The Seller [Naam] with full corporate authority and responsibility hereby certifies, represents and warrants that it is ready, willing and able to fulfill the requirements of this agreement and provide the product."

12. In the contract, Arshad listed his company's signatory as Q.S., which included the line "Read, approved and signed at [sic] [Q.S.] on 17 JANUARY 2022," and a photocopy of Q.S.'s passport. Information obtained during the course of this investigation indicates that Q.S. was a former employee of Naam located in Dubai.

13. Specifically, I obtained a WhatsApp chat from June 1, 2022, in which Q.S. communicated with another potential victim of Arshad, saying "please do not accept any document from him [Arshad] where he is using my signatures. I haven't signed any papers for this company [Naam] beyond sep 2021." Arshad strategically used the name, signature, and passport of Q.S., a former employee, to sign off on the contract with D.B.'s company.

14. After the contract had been finalized, Arshad requested that D.B.'s company send him an advance payment of \$55,000, which was to be used by Arshad to purchase a Performance Bond and obtain the shipping documents for the product. A Performance Bond (PB) is a financial guarantee issued by a bank or insurance company and provided by the seller to assure the buyer that if the commodity is not delivered, the buyer will still receive monetary compensation for the lost costs. It is uncommon practice for the obligee (D.B.'s company in this case) to provide the funds for the PB as it is generally the responsibility of the seller (Arshad in this case) to cover that risk. According to D.B., Arshad justified this request of advance funds by citing the global supply chain shipping crisis that was occurring in early 2022 that resulted in higher shipping costs.

15. D.B. agreed to send the advance to help secure the deal. Until D.B.'s company received the PB and the subsequent product shipping confirmation from Arshad, they could not move forward in the process to release the funds from the Letter of Credit from the Chinese companies. The shipping documents are required by the banks before funds will be released.

16. Arshad received the \$55,000 on February 8, 2022, which was wired to Naam's JPMorgan Chase Bank business checking account ending in -1689 ("Chase-1689") from the account of the financier used by D.B.'s company, Epsilon Acquisition Services (Epsilon), Bank of America account ending -9079. I obtained account statements for Chase-1689, which revealed the balance at the beginning of February 2022 as \$460.37. According to the bank records I reviewed, the same day that the money from Epsilon appeared in the account, Arshad transferred \$20,000 to his personal checking account with Chase Bank, account ending -9319 ("Chase-9319"). Over the next two days, Arshad transferred a total of \$30,000 to a Bank of America account in the name of a company called Lotus USA Inc¹. Two weeks later, an additional \$1,000 was transferred to Arshad's personal checking account. There is no indication that any of the \$55,000 from D.B.'s company was used to obtain the PB or shipping documents as agreed upon.

17. In a WhatsApp message on February 13, 2022, between Arshad, D.B., and other parties related to the contract, Arshad wrote, "Tomorrow we will have your PB issued." Despite this representation to D.B., Arshad did not obtain a PB the next day on February 14. When the PB was not produced by Arshad, D.B. reached out to him almost daily for two weeks. In response, Arshad blamed the bank for the failure to deliver the PB.

¹ Records obtained from Bank of America indicate that in 2023, an account owned by Lotus USA Inc. is pending closure.

18. A PB from Rakbank in UAE was finally produced by Arshad and received by D.B. on March 1, 2022. The bond guarantee amount was only for \$7,700, not the expected 10% of the value of the two contracts (approximately \$500,000). It is unclear what funds Arshad used to purchase this bond. D.B. continued to communicate with Arshad for the next six weeks attempting to resolve this glaring issue and salvage the contracts with the Chinese companies. Arshad, however, was uncooperative and continued to invent excuses for his failure to hold up his end of the contract.

19. On March 8, 2022, S.A., another commodities trader who had initially introduced D.B. and Arshad and who was also involved in the deal, wired Arshad \$24,980 of his personal funds to help salvage D.B.'s deal with Naam. This money was intended to help Arshad secure a suitable PB and the shipping documents, the lack of which precluded D.B.'s company from moving forward with the buyers. On March 8, 2022, Arshad received the aforementioned \$24,980 in his personal account, Chase-9319.

20. I obtained account statements from Chase-9319. The records show that the account had a negative balance of -\$238.41 on March 7, 2022, the day before the funds arrived. Within ten (10) days of the money from S.A. arriving in Arshad's account, the following financial activity can be seen taking place: (a) checks for \$4,000 and \$11,000 made out to Naveed Arshad; (b) \$3,976.12 sent via Western Union to UAE; (c) \$1,000 charge at a Mercedes-Benz dealership in Virginia; (d) a \$1,194.67 charge to Emirates Airlines; (e) a \$683.71 car payment; and (f) a \$570.05 payment for a personal loan that Arshad had taken out to cover medical/dental expenses.

21. I obtained a copy of an email thread with the subject title "FW: Naam – Refund of USD55,000.000" that was dated April 19, 2022, and exchanged between the Target Account and representatives from D.B.'s company. The original email was from D.B.'s company, requesting

Arshad refund the \$55,000 they had sent for the PB. The email further indicated that due to Arshad's lack of cooperation, the deal would no longer be moving forward. Arshad responded using the Target Account on the same day, accusing D.B.'s company of lying to him and providing him with falsified documents. This was nothing more than an excuse to justify Arshad's refusal to refund the money.

22. To date, Arshad has never refunded any of the money to D.B.'s company. Due to Arshad's conduct, D.B.'s company lost the two contracts with the Chinese companies valued at a combined \$6 million.

Loan from E.S.

23. In mid-2021, Arshad was introduced to E.S., the owner of a commodities business, through a mutual business associate. E.S. wanted to use Arshad as a seller for certain commodities for futures contracts, so Arshad began sending quotes, product specifications, and other documentation to E.S. The documentation provided by Arshad, including a Company Information Sheet (CIS), lists the Target Account as the company's email address.

24. E.S. was eager to foster a business relationship with Arshad, so when in March 2022 Arshad asked E.S. for a personal favor – a \$250,000 loan – E.S. was happy to oblige. Arshad told E.S. that he needed the loan because he did not have the liquidity to cover a Performance Bond, and he promised to repay the entire loan on or before the end of the month, March 31, 2022. On March 9, 2022, Arshad provided a promissory note to E.S. which indicated the terms of the loan repayment.

25. I obtained statements from the Chase-1689 Naam bank account. The statement shows a wire of \$250,231.00 from E.S.'s company to Arshad's Chase-1689 Naam bank account on March 14, 2022. The Chase-1689 account balance at the beginning of that month was \$7.90.

Once the loan money entered Arshad's account, Arshad transferred \$5,000 to his personal checking account (Chase-9319) and five (5) different wire transactions were sent to a company called Epsilon Acquisition Services LLC² ("Epsilon"), amounting to \$200,000:

- March 15, 2022 - \$45,000 to Epsilon;
- March 17, 2022 - \$45,000 to Epsilon;
- March 22, 2022 - \$45,000 to Epsilon;
- March 22, 2022 - \$50,000 to Epsilon; and
- March 24, 2022 - \$15,000 to Epsilon.

26. E.S. did not receive the loan repayment by the date Arshad promised. On April 3, 2022, E.S. sent a WhatsApp message to Arshad asking about the \$250,000. Arshad indicated he would wire the money on April 13, 2022. When that day came, Arshad asked E.S. if it would be possible to delay the repayment by one week, because Arshad needed to pay a supplier. As an incentive, Arshad would add \$10,000 to the amount owed, repaying E.S. \$260,000 in total. E.S. told Arshad that he needed that money in order to make payments on other contracts, but that E.S. could liquidate some positions in order to make that payment if need be. E.S. agreed to postponing the repayment for a week. On April 28, 2022, E.S. inquired about the \$260,000 repayment, to which Arshad did not reply.

27. E.S. continued to ask Arshad for his money back and Arshad continued to promise that E.S. would receive the wire on particular dates. These dates continued to come and go for several months with no wire. In a WhatsApp message from April 16, 2022, Arshad sent E.S. a

² Open-source research of Epsilon indicates it was a merger and acquisition advisory and investment group that is no longer in business.

screenshot of a Letter of Credit referencing Chase-1689 and told E.S. that he had \$8.2 million in his Chase account, which he would use to repay the loan. I obtained statements from this account, and this account has never had that much money, and at or around the time Arshad represented to E.S. that he had \$8.2 million, the account only had approximately \$8,500.

28. Following April 16, 2022, E.S. continued to request repayment from Arshad, as demonstrated by the below excerpts of communications between E.S. and Arshad on WhatsApp:

April 30, 2022, E.S.: Still no wire

May 1, 2022, E.S.: No wire yet

May 7, 2022, E.S.: Still no wire What is happening today?

May 7, 2022, Arshad: [E.S.] give me just two days Brother please. It is happening.

May 7, 2022, E.S.: So I can count on funds in my account on Monday?

May 7, 2022, Arshad: Keep it Tuesday for sure

May 7, 2022, E.S.: I absolutely have to have these funds by Tuesday, You are severely disrupting my business

May 11, 2022, Arshad: The delay is coming from the bank. I promise I have not put the money in any deal I used it for PB and got the LC in place. Just a delay on the banking side...The payment is stuck in compliance

May 11, 2022, E.S.: This will cause me a big problem tomorrow with my relationship with my supplier Itold [sic] him he would absolutely receive a wire tomorrow and now I only have a part of what I promised, With so much money in your accounts isn't there someone who would loan you this small amount?

May 12, 2022, E.S.: Didn't hear from you Still no wire

May 14, 2022, Arshad: I am waiting for the wire from Qatar to come in...It is scheduled today to hit the account.

May 15, 2022, Arshad: Don't worry your 260,000 will deposit Wednesday morning by all means

May 15, 2022, E.S.: You're giving me several absolute deadlines that you would have funds back to me and you have failed to do so on each deadline

May 15, 2022, Arshad: I will have you the funds by Wednesday by all Means. No more delay on anything

May 18, 2022, Arshad: I am shooting for Wednesday just on the safe side saying Thursday if my wire gets pending

May 21, 2022, E.S.: No wire has come in

May 22, 2022, E.S.: No wire today

May 22, 2022, Arshad: I am working on it

June 2, 2022, E.S.: Still no wire

June 2, 2022, Arshad: It should be with you by the end of this week without any delays

June 10, 2022, E.S.: No wire today

June 11, 2022, Arshad: By the end of the day or maximum tomorrow morning I will not let the weekend pass away without sending the money to you

June 15, 2022, E.S.: Are you wiring the funds today?

June 15, 2022, Arshad: I am waiting on the bank it should be all cleared today

June 17, 2022, E.S.: Still no wire...You promised today

June 17, 2022, Arshad: [E.S.] please I am doing it please please I am begging you give me some time please I am swearing on my kids I will get you the money please I just need one more day please I am begging you for it please

June 17, 2022, E.S.: [Arshad] You once again have failed to pay me as you promised. Therefore you have till 5pm EST June 17, 2022 to pay or I will be taking action.

June 17, 2022, Arshad: Ok agreed

June 19, 2022, Arshad: I tried and tried bank has not released me the funds Today also and Monday is a bank Holiday every thing has gone to next week

29. Arshad continually blamed the banks for his failure to repay the loan to E.S. On October 12, 2022, Arshad finally sent a \$10,000 wire to E.S. as a partial repayment of the loan. Since then, E.S. has not received any other money from Arshad.

Use of Target Account

30. The FBI has evidence of the Target Account being used to communicate with victim D.B. regarding D.B.'s company's business relationship with Arshad. And due to the Target Account being advertised as the company email address on multiple documents provided to Arshad's victims, including E.S., it is reasonable to believe that other communications containing evidence of the schemes exist in this account.

31. A preservation request to Google for the Target Account was made under 18 U.S.C. 2703(f) on April 24, 2023. In general, an email that is sent to a Google subscriber is stored in the subscriber's "mailbox" on Google servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on Google servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on Google's servers for a certain period of time.

BACKGROUND CONCERNING EMAIL

32. In my training and experience, I have learned that Google provides a variety of on-line services, including electronic mail (“email”) access, to the public. Google allows subscribers to obtain email accounts at the domain name @gmail.com or at custom domain names. Subscribers obtain an account by registering with Google. During the registration process, Google asks subscribers to provide basic personal information. Therefore, the computers of Google are likely to contain stored electronic communications (including retrieved and unretrieved email for Google subscribers) and information concerning subscribers and their use of Google services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

33. A Google subscriber can also store with the provider files in addition to emails, such as address books, contact or buddy lists, calendar data, pictures (other than ones attached to emails), and other files, on servers maintained and/or owned by Google. In my training and experience, evidence of who was using an email account may be found in address books, contact or buddy lists, email in the account, and attachments to emails, including pictures and files.

34. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and my experience, I know that, even

if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

35. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

36. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

37. As explained herein, information stored in connection with an email account may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct

under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user’s account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner’s state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner’s motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

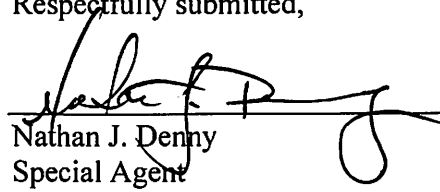
CONCLUSION

38. Based on the foregoing, there exists probably cause to search the information described in Attachment A for evidence, fruits, contraband, and/or instrumentalities of violations

of wire fraud (18 U.S.C. § 1343), as further described in Attachment B. Accordingly, I respectfully request that the Court issue the proposed search warrant.

39. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant. The government will execute this warrant by serving the warrant on Google. Because the warrant will be served on Google who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



Nathan J. Denny
Special Agent
FBI, Richmond Field Office
U.S. Department of Justice

Subscribed and sworn to before me on June 30, 2023.



Honorable Summer L. Speight
UNITED STATES MAGISTRATE JUDGE

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the email address naamcommodities@gmail.com that is stored at premises owned, maintained, controlled, or operated by Google LLC, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California 94043.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by Google LLC (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on **April 24, 2023**, the Provider is required to disclose the following information to the government for the account or identifier listed in Attachment A:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby ordered to disclose the above information to the government within **14 days** of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes evidence and fruits of violations of wire fraud (18 U.S.C. § 1343) involving Naam Commodities FZ LLC ("Naam") and Naveed Arshad ("Arshad") since in or around January 2021, including information pertaining to the following matters:

- (a) Information and correspondence related to Arshad and Naam;
- (b) Information and correspondence related to Arshad's relationship with and control of Naam;
- (c) Information and correspondence involving any individual employee or associate of Naam, including, but not limited to, Q.S., as it relates to that individual's actions on behalf of or while employed by either Arshad or Naam;
- (d) Information and correspondence related to actual and potential customers and business partners of Naam, including, but not limited to, information regarding the solicitation of potential customers;
- (e) Information and correspondence related to quotes, contracts, invoices, personal investments, and loans with buyers, sellers, or intermediaries received or provided by Arshad and his companies;
- (f) Information and correspondence related to the business dealings of Arshad and Naam Commodities, to include, but not limited to, correspondence with employees of those entities, bank accounts, finances, purchases of Performance Bonds, and the use and transfers of funds;

- (g) Evidence indicating how, when, and where the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (h) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation; and
- (i) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts located anywhere in the United States. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not

potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. This investigation is presently covert and the government believes that the subject of the search is not aware of this warrant.